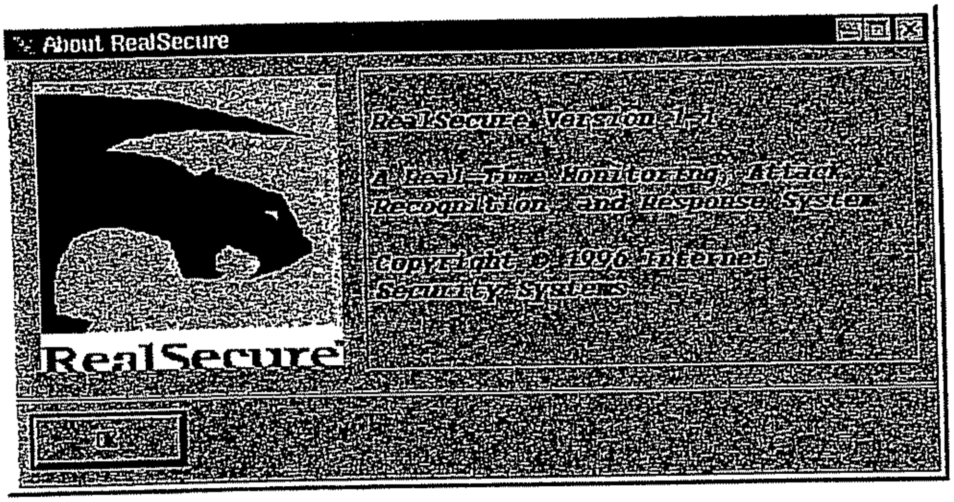
EXHIBIT H

INTERNET SECURITY SYSTEMS

More About RealSecure™

JOIN A MAIL LIST
JOIN AN ISS CHAT
DOWNLOAD NOW
SECURITY IQ

ABOUT ISS | NEWS & EVENTS | PRODUCTS | PARTNERS | TRAINING & SUPPORT | SECURITY LIBRARY | SEARCH | SITE MAP



RealSecure Version 1.1

A Real-Time Monitoring, Attack Recognition and Response System

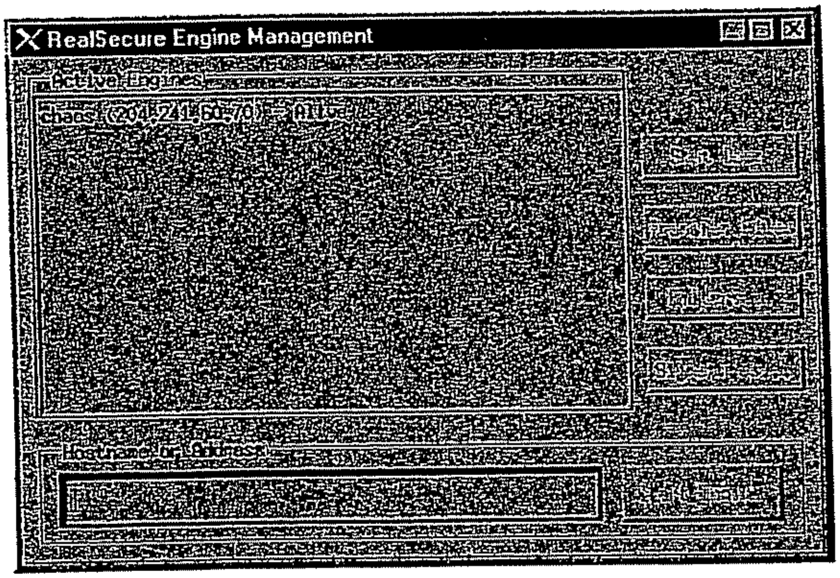
Copyright © 1996 Internet Security Systems

General Description and Comparison to Existing Systems

RealSecure™ was designed to manage the large amounts of data processed by a network in a manner not normally utilized by other network security products. Its configurability and many features make it useful for everything from logging hacking attempts to providing a second line of defense behind a firewall. It can detect and then report network events through various means including email or a user-written program. It can actively defend against attacks by closing attempted connections to your network. What really makes it different from every other network monitoring product is that it is designed to be an enterprise-wide solution, monitoring the company's network at many different points of failure 24 hours a day, 7 days a week.

RealSecure™ is composed of two parts: a filtering engine that watches and actively manages the network and a GUI front-end that reports events and allows the user to configure the engine's scope. Multiple engines can be run on machines near critical points in the network, such as the firewall or a sensitive LAN. The engines report interesting data back to the GUI and automatically handle certain events which the administrator wishes to prevent or track. The engine runs on SunOS, Solaris, and Linux (right now) and doesn't require too much in the form of system resources. Lots of disk space is good for allowing logging, and more performance is better if the network traffic to be monitored is heavy. The GUI can run on the same platforms, but requires more performance and a graphical display. This makes the GUI best suited for use on a dedicated administrative machine. In fact, it is recommended that any machine running the GUI or the engine be dedicated to that purpose for performance and security reasons.

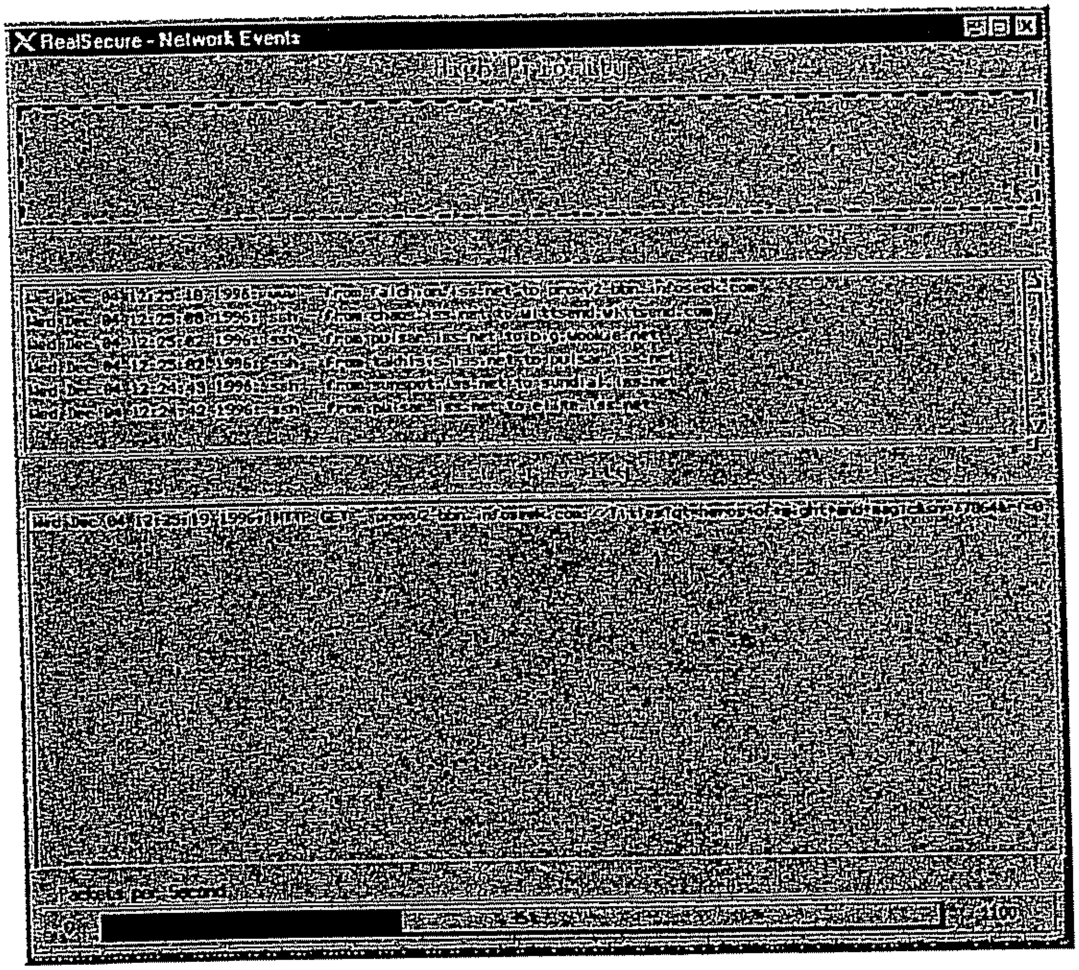
Starting the GUI shows a short intro screen and then presents the user with the startup window. This window is used to start engines, configure them, and retrieve log files from engines. To start an engine, the user simply types in the name or IP of the machine on which to run the engine. By clicking on an engine in the list, he can also change the configuration info for that engine, shut it down, or fetch files from that machine.



chaos (204.241.60.70)

Figure 1 - RealSecure™ Configure Engines Screen

When the user starts an engine, he is presented with a screen which shows a short summary of events classified by security priority: High, Medium, and Low. At the bottom of the screen is a bar graph showing the packets received per second, with the label indicating the maximum ever received. The top menu bar has buttons to load a config file, pop up the GUI configuration editor, or get help.



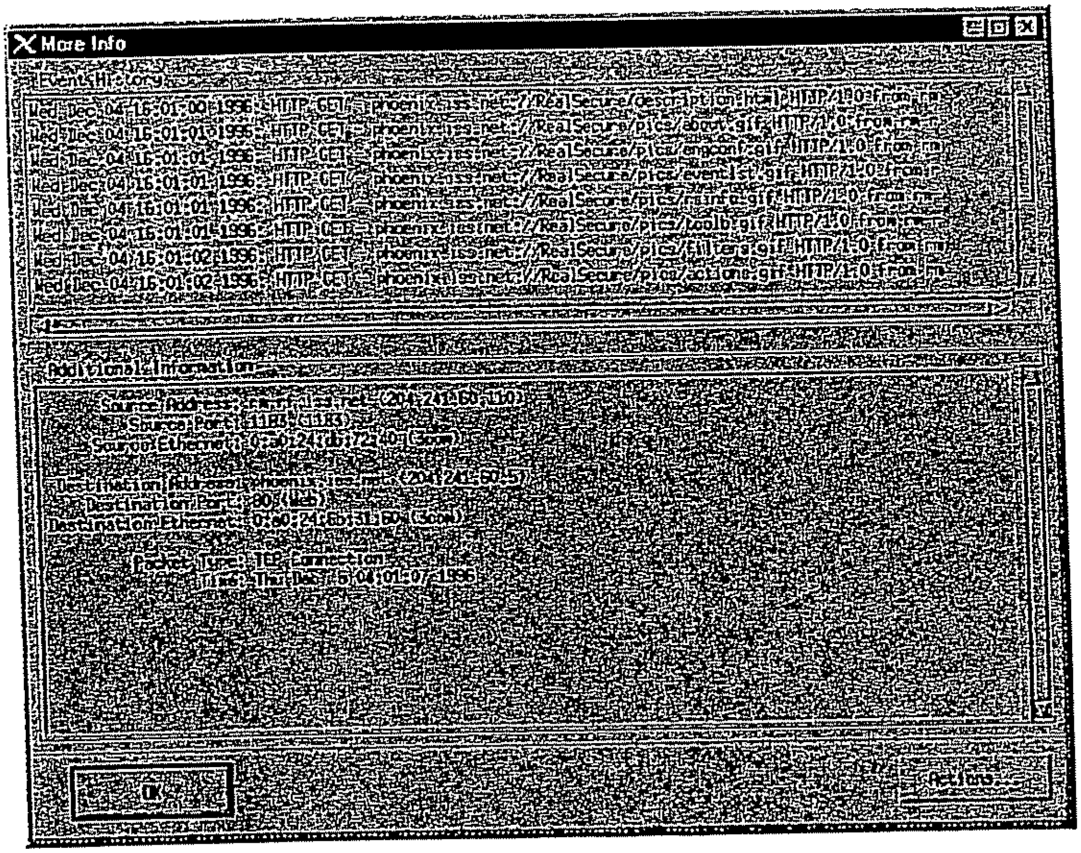
```
Wed Dec 04 12:25:10 1996: www -- from [illegible].iss.net to proxy2-bbn.infoseek.com
Wed Dec 04 12:25:08 1996: ssh -- from chaos.iss.net to [illegible]
Wed Dec 04 12:25:02 1996: ssh -- from pulsar.iss.net to [illegible]
Wed Dec 04 12:25:02 1996: ssh -- from [illegible].iss.net to pulsar.iss.net
Wed Dec 04 12:24:49 1996: ssh -- from sunspot.iss.net to sundial.iss.net
Wed Dec 04 12:24:42 1996: ssh -- from pulsar.iss.net to [illegible]
```

```
Wed Dec 04 12:25:19 1996: HTTP GET -- proxy2-bbn.infoseek.com [illegible]
```

Figure 2 - RealSecure™ Main Screen

As events occur on the network, the engines send messages to the gui to indicate the event and the level. The gui displays them according to priority. The user can double-click on an event in any of the three windows, and then select some action to be performed on that event. At the moment, he can select "More Info", "Log", "View", or "Kill". What that action actually does is limited to the type of event. For instance, if a user decided to log all name queries (DNS), and then tried to kill one of them, it wouldn't be possible because the query would already be finished and there would be no connection to close.

Bringing up the "More Info" window queries the engine for more information about the selected event. This can include items like the source of the packet or perhaps some of the data from the packet like email headers or other important data to log. Its use is to allow the administrator to make a decision whether to ignore the event or take some kind of action.



```
Wed Dec 04 16:01:00 1996: HTTP GET - phoenix.iss.net://RealSecure/description.html HTTP/1.0 from rn
Wed Dec 04 16:01:01 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/about.gif HTTP/1.0 from rn
Wed Dec 04 16:01:01 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/engconf.gif HTTP/1.0 from rn
Wed Dec 04 16:01:01 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/eventlst.gif HTTP/1.0 from r
Wed Dec 04 16:01:01 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/rsinfo.gif HTTP/1.0 from rn
Wed Dec 04 16:01:01 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/toolb.gif HTTP/1.0 from rn
Wed Dec 04 16:01:02 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/filters.gif HTTP/1.0 from rn
Wed Dec 04 16:01:02 1996: HTTP GET - phoenix.iss.net://RealSecure/pics/actions.gif HTTP/1.0 from rn
```

```
     Source Address: [illegible].iss.net (204.241.60.110)
        Source Port: 1183 (1183)
    Source Ethernet: 0:a0:24:db:72:40 (3com)
Destination Address: phoenix.iss.net (204.241.60.5)
   Destination Port: 80 (Web)
Destination Ethernet: 0:a0:24:8b:31:60 (3com)
        Packet Type: TCP Connection
               Time: Thu Dec 5 04:01:07 1996
```

Figure 3 - More Info Screen

The "View" window decodes the data for a given connection into a nice, usable format appropriate for the given connection. For starters, it will show a telnet, rlogin or interactive rsh session in a window with the user's keystrokes in the bottom window. What's nice about this is that the screen looks exactly like what the hacker sees, making it simple to make a decision whether or not to take further action. This can also be used to help network users when they are having problems. The administrator can go on to log or kill the session from this window. The view window looks the same as the playback window described below.

Logging data can be done automatically or manually triggered by the user. Data can be saved in raw format for later playback, or just the pertinent data like where the connection is from can be logged. Logs can be in text format as well for easy perusal or insertion in reports.

The toolbar appears with the engine config screen. It allows quick access to the main components of RealSecure.

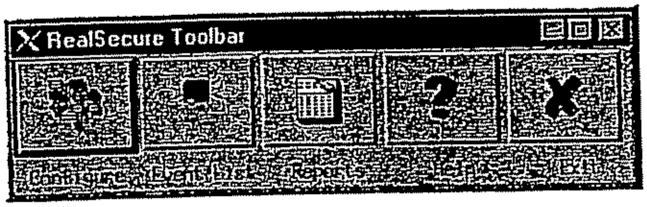


Figure 4 - Toolbar

The most important feature of RealSecure™ is its configuration screen, which allows the user to easily tailor a model of the network and prepare custom checks and responses.

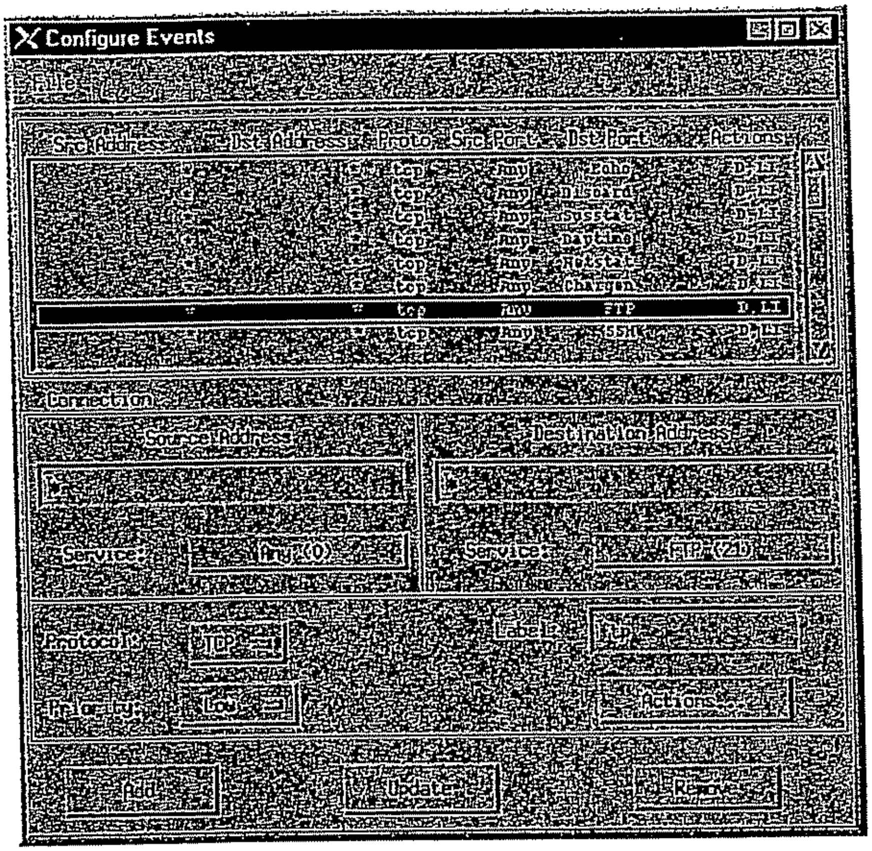
```
# Format:
#     Source Address     Dest Address       S Port  D Port Tag    Pri    Action
tcp          129.65.0.0/16    10.0.1.8/32         0       23    Login   1     K,LR=data
```

Figure 5 - Sample filter configuration entry

While this may seem complex, it's easy to understand with a little explanation. This rule takes all TCP packets from 129.65.* (any port) sent to the single machine 10.0.1.8 (port 23) and kills the connection and logs all the data it can about the connection. It is assigned a priority of "high", meaning its notification will appear in the high priority window of the main screen (see Figure 1). The tag will also appear in the window, allowing an administrator to easily pick out which events fit the same categories.

The source and destination address format may be unfamiliar to those who have never configured a firewall. It has two components: the address to match and the number of bits to match from it. All IP's are 32 bits, with each of the dotted numbers signifying eight of those bits. So, 205 is eight bits, 205.16 is sixteen bits, 205.16.18 is twenty-four bits, and lastly, 205.16.18.2 is thirty-two bits. To match all machines coming from 205.16.18.X (where X is some number), the rule would be 205.16.18.0/24. This rule would match 205.16.18.1 and 205.16.18.233, but not 205.16.17.1.

Remember that most users will not have to deal with this config file format, but it's there for those who want to customize the filters very specifically for their network. Most users will probably be using the GUI config, which allows much of the same functionality, but in a bit more friendly manner. For instance, the rule above would be created in the GUI configuration by selecting your network address as 10.0.1.*, selecting a source address of 129.65.*, saying to log and kill all TCP connects to your telnet port.



Src Address	Dst Address	Proto	Src Port	Dst Port	Actions
*	*	tcp	Any	Echo	D,LI
*	*	tcp	Any	Discard	D,LI
*	*	tcp	Any	Sysstat	D,LI
*	*	tcp	Any	Daytime	D,LI
*	*	tcp	Any	Netstat	D,LI
*	*	tcp	Any	Chargen	D,LI
*	*	tcp	Any	FTP	D,LI
*	*	tcp	Any	SSH	D,LI

Source Address: *
Service: Any (0)

Destination Address: *
Service: FTP (21)

Protocol: TCP
Label: ftp
Priority: Low
Actions

Figure 6 - Filters Configuration Screen

Both the attack signatures config and the filter rules config have a certain set of actions (responses) available for the user to use interactively or the engine to use automatically.

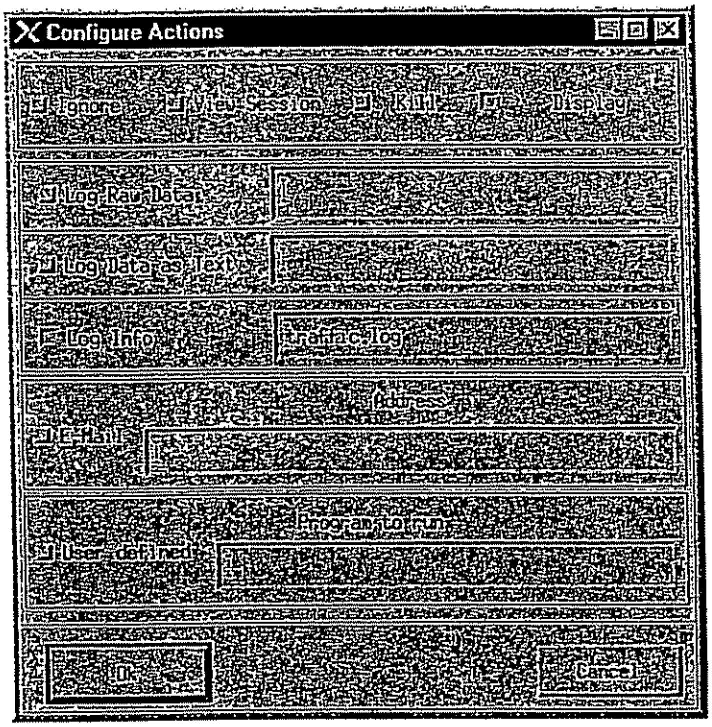


Figure 7 - Actions Configuration Screen

All the different attack signatures are configured through this next screen. Signatures can be enabled or disabled, the log messages can be editted, and any associated actions can be configured. Also, any signature which has tunable parameters (to prevent false alarms) can be managed from this screen.

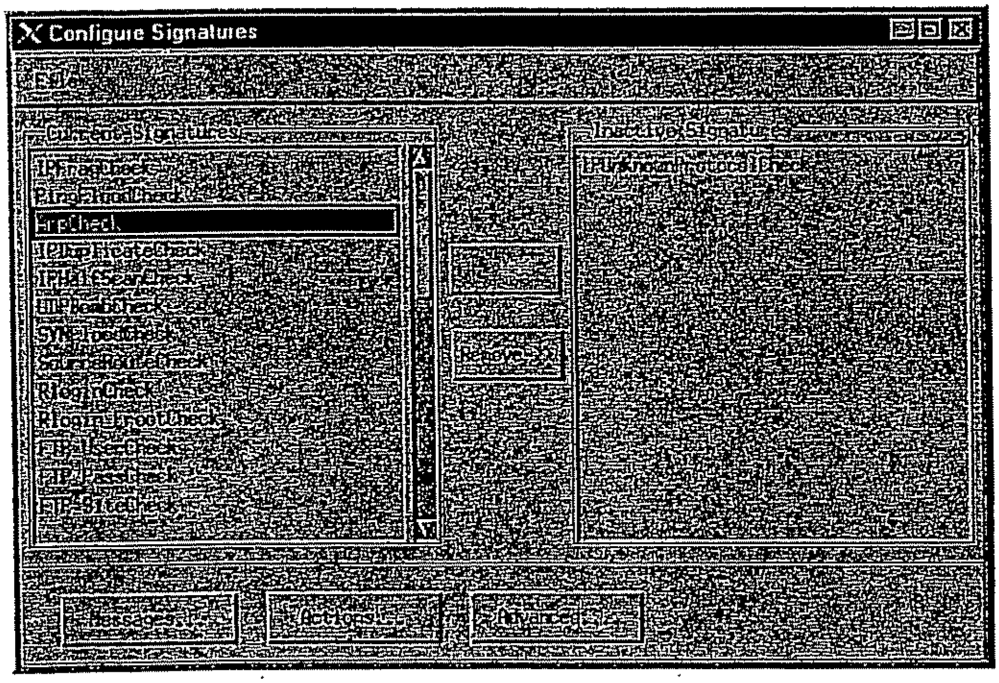
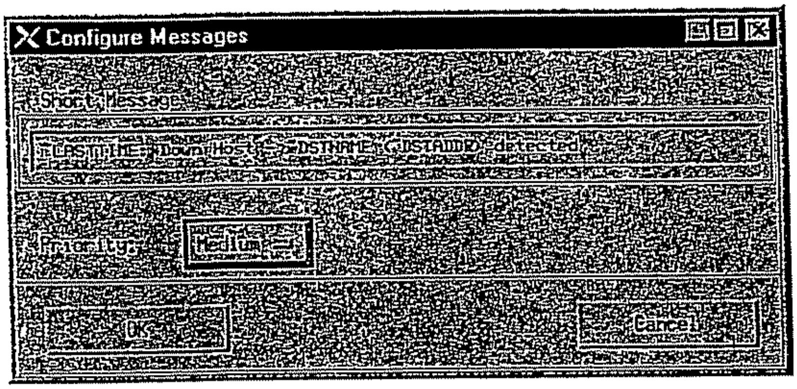


Figure 8 - Attack Signatures Configuration Screen

Users can configure the messages and the priority that they appear at by using the config messages dialog.



Configure Messages

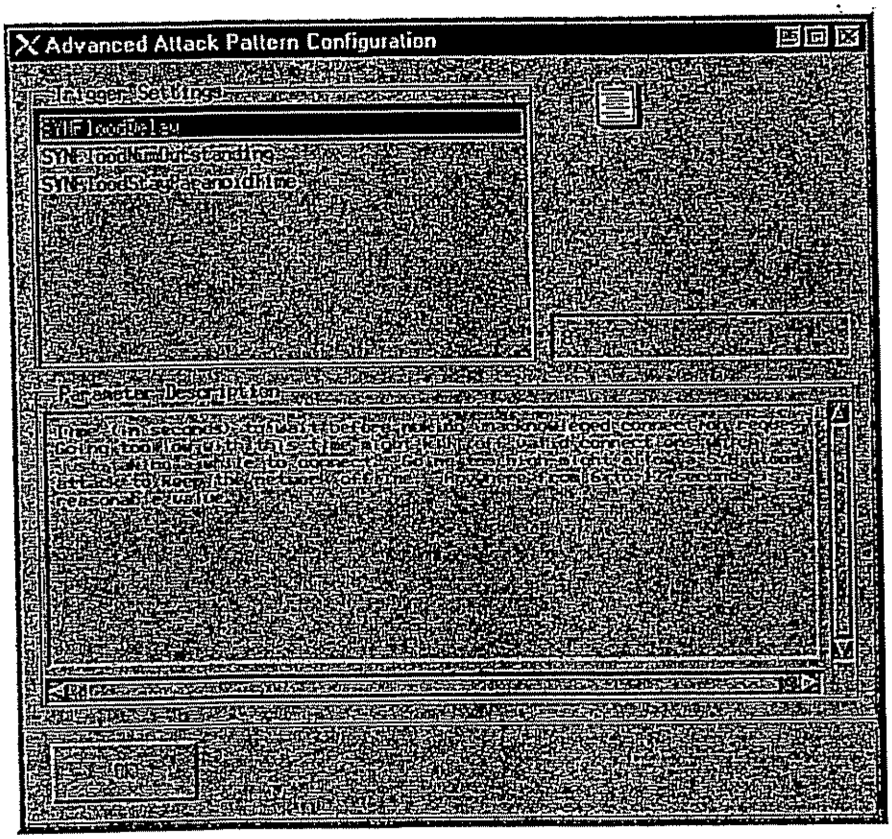
Short Message

[LASTTIME] Down Host <DSTNAME (DSTADDR) detected

Priority: Medium

Figure 9 - Messages Configuration Screen

Some signatures have advanced config options which allow them to be custom-tuned for a network. This prevents false positives and makes RealSecure™ a more effective monitoring tool. Here is a picture of a user configuring the SYN Flood Check.



Advanced Attack Pattern Configuration

Trigger Settings

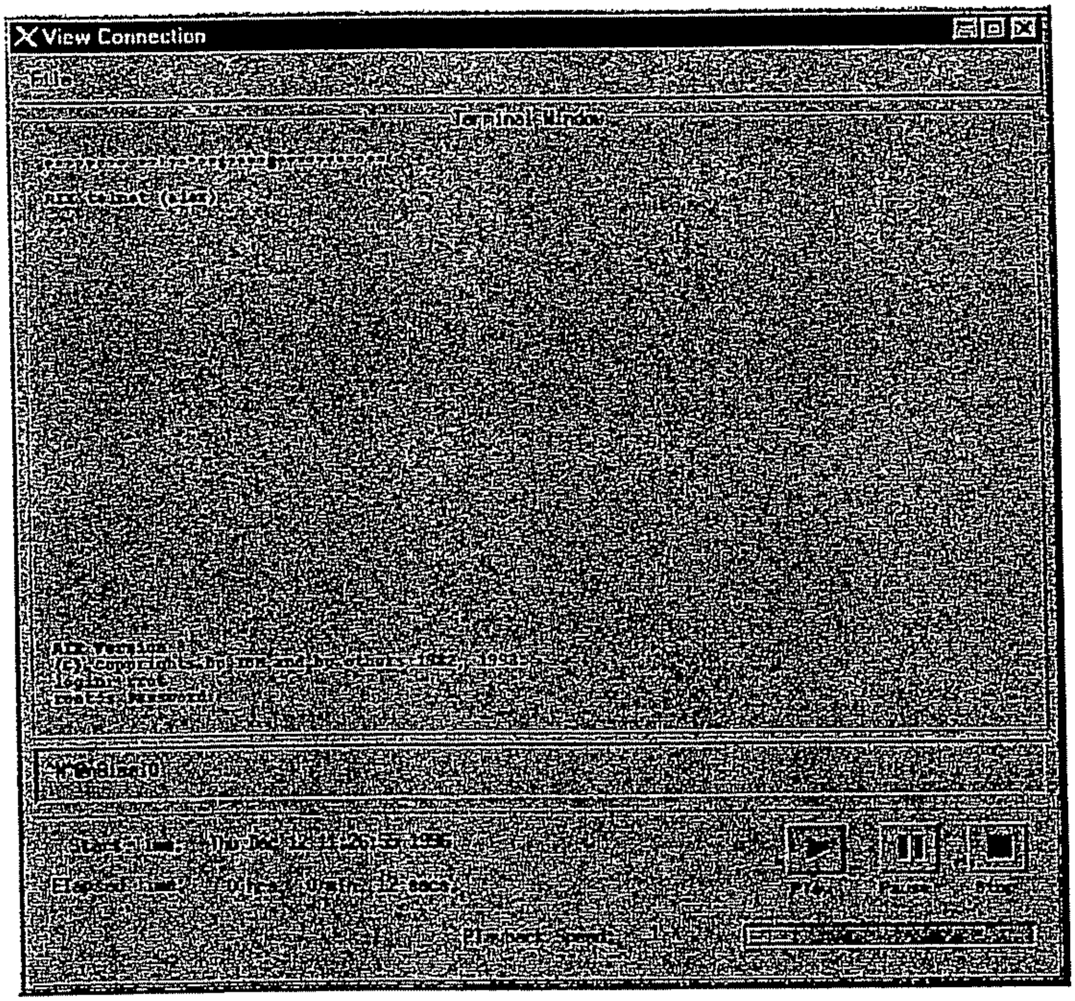
SYNFloodDelay
SYNFloodNumOutstanding
SYNFloodStagnantOldTime

Parameter Description

Time (in seconds) to wait before [illegible] unacknowledged connection request. Going too low [illegible] valid connections [illegible] to connect [illegible] attack to keep the network off line [illegible] from 6 to 12 seconds [illegible] reasonable value.

Figure 10 - Advanced Signature Configuration Screen

The playback utility gives a VCR-like interface for replaying logged data. The user can select a log file and then play back the session in real-time. The playback can be paused at any time, or sped up and slowed down. The seek buttons allow the user to jump to the next recorded session. The screen also displays informational messages about the connection.



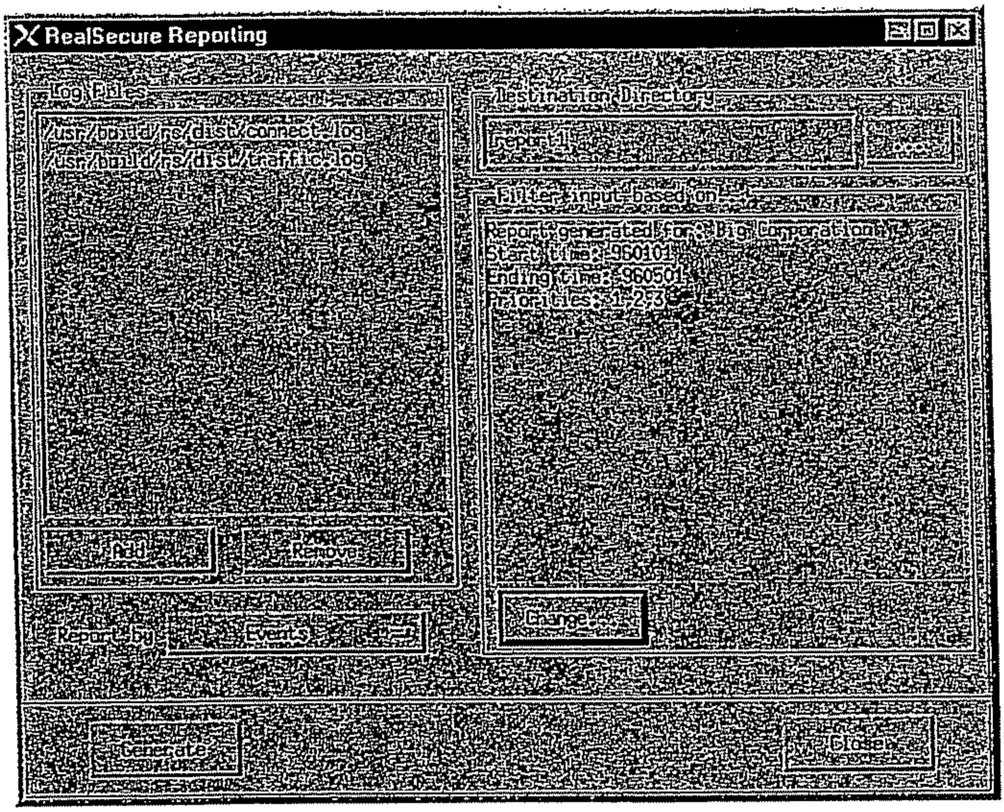
```
[illegible]
AIX telnet (xlax)

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1993.
login: root
root's Password:
```

Start Time: Thu Dec 12 11:26:53 1996
Elapsed Time: 0 hrs 0 min 12 secs

Figure 11 - Playback Screen

The report generation screen allows the user to choose the type of report he wants, as well as what files to use to generate the report.



Log Files

/usr/build/rs/dist/connect.log
/usr/build/rs/dist/traffic.log

Report by: Events

Destination Directory: report1

Filter input based on:

Report generated for: Big Corporation
Start time: 960101
Ending time: 960501
Priorities: 1,2,3

Figure 12 - Report Screen

Sales Inquiries: info@iss.net

41 Perimeter Center East · Suite 660 · Atlanta, GA 30346 · (770) 395-0150 · (770) 395-1972 FAX